

01-31-06

TFW

2611

BEST AVAILABLE COPY



PTO/SB/21 (09-04)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>	Application Number	09/400,447-Conf. #3453
	Filing Date	September 21, 1999
	First Named Inventor	Jean-Paul Bastien
	Art Unit	2611
	Examiner Name	H. B. Lonsberry
Total Number of Pages in This Submission	Attorney Docket Number	11345/102001

ENCLOSURES (Check all that apply)

<input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input checked="" type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Reply to Missing Parts/Incomplete Application <input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____ <input type="checkbox"/> Landscape Table on CD	<input type="checkbox"/> After Allowance Communication to TC <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input checked="" type="checkbox"/> Other Enclosure(s) (please identify below): Return Receipt Postcard
<div style="border: 1px solid black; padding: 5px; min-height: 40px;"> Remarks </div>		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	OSHA · LIANG LLP		
Signature			
Printed name	Jonathan P. Osha THOMAS SCHERER		
Date	January 30, 2006	Reg. No.	33,986

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV841966996US, on the date shown below in an envelope addressed to:
 Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Dated: January 30, 2006

Signature

(Michelle Hayden)

THIS PAGE BLANK (USPTO)



I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV841966996US, on the date shown below in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Dated: January 30, 2006

Signature: *Michelle Hayden*

(Michelle Hayden)

Docket No.: 11345/102001
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Jean-Paul Bastien et al.

Application No.: 09/400,447

Confirmation No.: 3453

Filed: September 21, 1999

Art Unit: 2611

For: BROADCAST AND RECEPTION SYSTEM,
AND RECEIVER/DECODER AND REMOTE
CONTROLLER THEREFOR

Examiner: H. B. Lonsberry

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants hereby claim priority under 35 U.S.C. 119 based on the following
prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
European Patent Office	97400650.4	March 21, 1997

In support of this claim, a certified copy of the said original foreign application is
filed herewith.

THIS PAGE BLANK (USPTO)

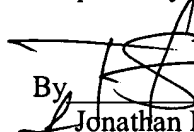
Application No.: 09/400,447

Docket No.: 11345/102001

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-0591, under Order No. 11345/102001 from which the undersigned is authorized to draw.

Dated: January 30, 2006

Respectfully submitted,

By  #45,079
Jonathan P. Osha THOMAS SCHERER
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)

THIS PAGE BLANK (USPTO)



Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr.

Patent application No.

Demande de brevet n°

97400650.4 / EP97400650

The organization code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP97400650

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R.C. van Dijk

THIS PAGE BLANK (USPTO)



Anmeldung Nr:
Application no.: 97400650.4
Demande no:

Anmeldetag:
Date of filing: 21.03.97
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

CANAL+ Société Anonyme
85/89 Quai André Citroën
75711 Paris Cedex 15/FR

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se référer à la description.)

Broadcast and reception system

In anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation / International Patent Classification / Classification internationale de brevets:

Am Anmeldetag benannte Vertragsstaaten / Contracting states designated at date of filing / Etats contractants désignées lors du dépôt:

AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

THIS PAGE BLANK (USPTO)

BROADCAST AND RECEPTION SYSTEM

The present invention relates to a broadcast and reception system, in particular to a mass-market digital interactive satellite television system.

5 Claimed herein as the present invention are any or all of the novel and inventive features described herein, in particular any of all of the section, sub-section or sub-sub-section headings which are claimed as the present invention.

Preferred features of the present invention will now be described, purely by way of example, with reference to the accompanying drawings, in which:-

10 Figure 1 shows the overall architecture of a digital television system according to the preferred embodiment of the present invention;

Figure 2 shows the architecture of a conditional access system of the digital television system;

15 Figure 3 shows the arrangement of memory zones in a smartcard of the conditional access system;

Figure 4 is a schematic diagram of a remote controller used in the digital television system;

Figure 5 shows the architecture of an interactive system of the digital television system;

20 Figure 6 shows the arrangement of files within a module downloaded into the memory of an interactive receiver decoder;

Figure 7 shows the arrangement of memory volumes of the memory of the

interactive receiver decoder;

Figure 8 is a schematic diagram of interfaces of the receiver decoder;

Figure 9 is a schematic diagram of an Authoring Tool of the interactive television system;

- 5 Figure 10 is a schematic diagram of a Broadcasting Application and Server of the interactive television system; and

Figure 11 shows the architecture of the software in the receiver decoder.

An overview of a digital television system 1000 according to the present invention is shown in Figure 1. The invention includes a mostly conventional
10 digital television system 2000 which uses the known MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 2002 in a broadcast centre receives a digital signal stream (typically a stream of video signals). The compressor 2002 is connected to a multiplexer and scrambler 2004 by linkage 2006. The multiplexer 2004
15 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 2008 of the broadcast centre via linkage 2010, which can of course take a wide variety of forms including telecom links. The transmitter 2008 transmits electromagnetic signals via uplink 2012 towards a satellite transponder 2014, where they are
20 electronically processed and broadcast via notional downlink 2016 to earth receiver 2018, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 2018 are transmitted to an integrated receiver decoder 2020 owned or rented by the end user and connected to the end user's television set 2022. The receiver decoder 2020 decodes the
25 compressed MPEG-2 signal into a television signal for the television set 2022.

- 3 -

A conditional access system 3000 is connected to the multiplexer 2004 and the receiver decoder 2020, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of
5 deciphering messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver decoder 2020. Using the decoder 2020 and smartcard, the end user may purchase commercial offers in either a subscription mode or a pay-per-view mode.

10 An interactive system 4000, also connected to the multiplexer 2004 and the receiver decoder 2020 and again located partly in the broadcast centre and partly in the decoder, enables the end user to interact with various applications via a modemmed back channel 4002.

The conditional access system 3000 and interactive system 4000 are now
15 described in more detail.

1. CONDITIONAL ACCESS SYSTEM

With reference to Figure 2, in overview the conditional access system 3000 includes a Subscriber Authorization System (SAS) 3002. The SAS 3002 is connected to one or more Subscriber Management Systems (SMS) 3004, one
20 SMS for each broadcast supplier, by a respective linkage 3006. First ciphering units 3008 utilising "mother" smartcards 3010 are connected to the SAS by linkage 3012. Second ciphering units 3014 utilising mother smartcards 3016 are connected to the multiplexer 2004 by linkage 3018. The receiver decoder 2020 receives a "daughter" smartcard 3020. It is connected directly to the
25 SAS 3002 by communication servers 3022 via the modemmed back channel 4002.

The operation of the conditional access system 3000 of the digital television

- 4 -

system will now be described in more detail with reference to the various components of the television system 2000 and the conditional access system 3000.

1.1. Multiplexer and Scrambler

- 5 In the broadcast centre, the digital video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 2002. This compressed signal is then transmitted to the multiplexer and scrambler 2004 via the linkage 2006 in order to be multiplexed with other data, such as other compressed data.

- 10 The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer 2004. The control word is generated internally and enables the end user's integrated receiver decoder 2020 to descramble the program.

- Access criteria, indicating how the program is commercialised, are also added to the MPEG-2 stream. The program may be commercialised in either a
15 "subscription mode" or a "pay per view (PPV) mode". In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels. In the pay per view mode, the end user
20 is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode").

- Both the control word and the access criteria are used to build an Entitlement Control Message (ECM). The access criteria and control word are transmitted
25 to the second ciphering unit 3014 via the linkage 3018. In this unit, a ECM is generated, ciphered and transmitted on to the multiplexer 2004.

1.2. Subscriber Management System (SMS)

A Subscriber Management System (SMS) 3004 includes a database 3024 which manages, amongst others, all of the end user files, commercial offers (such as tariffs and promotions), subscriptions, PPV details, and data
5 regarding end user consumption and authorization. Each SMS 3004 transmits messages to the SAS 3002 via respective linkage 3006 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

The EMM is a message, or unique address, dedicated to one end user, or a
10 group of end users, only (in contrast with an ECM, which is dedicated to one scrambled program only). The unique address, which consists of a group number and a position within the group, allows access by several end users using the same message. Each group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth, that is,
15 access to one group can permit the reaching of a great number of end users.

The SMS 3004 also transmits messages to the SAS 3002 which imply no modifications or creations of EMMs but implying only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

20 1.3. Subscriber Authorization System (SAS)

The messages generated by the SMS 3004 are passed via linkage 3006 to the Subscriber Authorization System (SAS) 3002, which in turn generates messages acknowledging receipt of the messages generated by the SMS 3004 and passes these acknowledgements to the SMS 3004.

25 One function of the SAS 3002 is to manage the access rights to television

programs, available as commercial offers and sold according to different modes of commercialisation (subscription mode, pre-book mode, impulse mode). The SAS 3002, according to those rights and to information received from the SMS 3004, generates EMMs for the subscriber. These generated
5 EMMs are passed as electrical signals to the first ciphering unit 3008, where they are ciphered and passed back to the SAS 3002.

The first and second ciphering units 3008 and 3014 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 3010 and 3016 respectively, referred to as a
10 "mother" smartcard, for each electronic card and which ciphers either the ECMs or the EMMs.

1.4. Program Transmission

The multiplexer 2004 receives electrical signals comprising ciphered EMMs from the SAS 3002, ciphered ECMs from the second ciphering unit 3014 and
15 compressed programs from the compressor 2002. The multiplexer 2004 scrambles the programs and transmits the scrambled programs, the ciphered ECMs and the ciphered ECMs as electric signals to a transmitter 2008 of the broadcast centre via linkage 2010. The transmitter 2008 transmits electromagnetic signals towards the satellite transponder 2014 via uplink 2012.

1.5. Program Reception

The satellite transponder 2014 receives and processes the electromagnetic signals transmitted by the transmitter 2008 and transmits the signals on to the earth receiver 2018, conventionally in the form of a dish owned or rented by the end user, via downlink 2016. The signals received by receiver 2018 are
25 transmitted to the integrated receiver decoder 2020 owned or rented by the end user and connected to the end user's television set 2022. The receiver decoder 2020 demultiplexes the signals to obtain scrambled programs with

ciphered ECMs and ciphered ECMs.

If the program is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver decoder 2020 decompresses the data and transforms the signal into a video signal for transmission to television set 2022.

5 If the program is scrambled, the receiver decoder 2020 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 3020 of the end user. This slots into a housing in the receiver decoder 2020. The daughter smartcard 3020 controls whether the end user has the right to decipher the ECM and to access the program. If not,
10 a negative status is passed to the receiver decoder 2020 to indicate that the program cannot be descrambled. If the end user does have the rights, the ECM is deciphered and the control word extracted. The decoder 2020 can then descramble the program using this control word. The MPEG-2 stream is decompressed and translated into a video signal for onward transmission to
15 television set 2022.

1.6. Smartcards

1.6.1. Multiple public keys stored in RAM

With reference to Figure 2, the memory in the daughter smartcards 3020 is divided into up to 16 independent memory zones 3026 containing their own
20 data.

The identifier of the smartcard is unique and stored in a separate reserved memory zone 3028.

Each remaining zone 3030 may be dedicated to one broadcast supplier. Where the end user has a subscription relating to a particular broadcast
25 supplier, the relevant zone 3030 of the daughter smartcard 3020 comprises the

following constant values:

- a broadcast supplier identifier; and

- secret keys of the broadcast supplier, allowing the receiver decoder 2020 to decipher the EMMs pertaining to the broadcast supplier.

5 **1.6.2. Temporary RAM key**

1.6.3. Dynamic creation of zones

The relevant memory zones 3030 of the smartcard may be dynamically created.

1.6.4. Selective dis-ablement of public keys

10 The relevant memory zone 3030 also includes the following dynamically variable value:

- a number of the group to which the smartcard 3020 belongs, and position of the smartcard 3020 in the group in order to access the smartcard 3020 with a group address. These values can be changed dynamically by
15 messages from the SAS 3002 in order to optimise the fragmentation of the groups;

- keys which are sent by the SAS along with a renewal EMM on a regular, preferably monthly, basis in order that the receiver decoder 2020 is able to decipher the ECM;

20 the obsolescence date of the keys;

- a subscription bitmap comprising the commercial offers to which the end user has subscribed;

- a "wallet" containing "tokens" used by the end user whenever he wants to watch a particular event and at the very moment that the event is broadcast,
25 and a limit under which it is no longer possible to purchase a particular event during impulsive viewing; and

- pointers in a global memory in the smartcard for PPV events. Those

- 9 -

events are stored in the smartcard 3020 within a specific memory, shared among the different zones 3026. For each event, the identifier of the session, the date of broadcasting and the number of tokens if purchased in impulsive mode are stored in the zone. In the preferred embodiments, the smartcard
5 3020 can store from 235 to 300 PPV events, according to the configuration of the smartcard.

1.6.5. Multi-broadcasting with decremental maximum number counter on smartcard

10 Assume that the daughter smartcard 3020 has the right to decipher the ECM received by the receiver decoder 2020 (and a future obsolescence date).

In respect of subscription television programs the receiver decoder 2020, having received a signal that it has the right to decipher the ECM, decipheres the ECM and checks whether the received access criteria contained in the deciphered ECM correspond to a number in the commercial offers subscription
15 bitmap in the relevant zone 3030 of the smartcard 3020. If so, the control word is extracted from the ECM to enable descrambling of the television program.

In respect of PPV mode, the receiver decoder 2020 determines whether the program is one sold in PPV mode. If so, the decoder 2020 checks, using the
20 pointers stored in the global memory of the relevant zone 3030 of the smartcard 3020, whether the session identifier for the program is stored therein. If the session identifier is stored therein, the control word is extracted from the ECM.

If the session identifier is not stored therein, by means of a specific application
25 the receiver decoder 2020 displays a message to the end user indicating that he has the right to view the session at a cost of, say, 25 tokens. If the end user answers "yes" (by means of remote controller 2026) the decoder 2020

decreases the wallet of the smartcard 3020 by 25 tokens, writes the identifier of the session in the global memory and extracts the control word from the ECM.

- 5 The access criteria may also include a session index; if the session is broadcast several times, this index can be set to differentiate one broadcast from the other. This feature permits authorization to be given for a subset of broadcasts, for example, 3 times out of 5 broadcasts. Each time this authorization is given, the number of the number counter is decreased by one.

1.6.6. Diversification

- 10 The unique address of the ciphered EMM produced using the mother smartcard 3010 can only be deciphered by one daughter smartcard or a group of similar smartcards. A diversification algorithm determines the EMM to be ascribed to a particular end user such that there can be no duplication of the EMM within, for example, a specific geographic location.

15 1.6.7. Qui Êtes Vous (QEV) function; smartcard/decoder pairing via a handshake

A Qui Êtes Vous (QEV) function is used to protect receiver decoders 2020 which have been bought by one broadcast supplier against the use of non-authorized daughter smartcards 3020.

- 20 In more detail, the receiver decoder 2020 contains a QEV value, preferably implemented as a number inside the memory 2024 of the decoder 2020 and set therein by the manufacturer. The memory zone 3028 of the smartcard 3020 contains a field or bitmap describing the categories of decoders 2020 with which it can function and which can be specified during the
25 personalization process of the smartcard 3020, as well as by a specific EMM. The decoder 2020 checks whether the inserted smartcard 3020 has a bitmap

which identifies with the QEV value of the decoder 2020.

1.7. Communication Servers

1.7.1. Communications Server connected directly to the SAS

5 The communication servers 3022 receive signals from the end user, either via
a command on a telephone or via the modemmed back channel 4002
connected to receiver decoder 2020, and transmits the signals directly to the
SAS 3002.

10 In the first mode the SAS 3002 processes the end user commands received
(in voice mode) as electric signals in the same way as commands received
from the SMS 3004. Messages are generated by the SAS 3002 and passed
to the multiplexer 2004.

1.7.2. Posting EMMs via the modemmed back channel

15 In the second mode, the receiver decoder 2020 is connected to the
communication servers 3022 by means the modemmed back channel 4002.
In this case, the commands are processed by the SAS 3002, messages
generated and then sent back directly to the decoder 2020 by means of the
back channel. In the case of pre-book mode, for example, the SAS 3002
receives messages from the end user requesting access to a specific event via
the modem and telephone line and returns a suitable EMM to the decoder
20 2020 via the modem and telephone line, that is, without having to transmit the
EMM in an MPEG-2 data stream via the multiplexer and scrambler 2004, to
enable the end user to view the event.

1.8. Remote Controller

1.8.1. Encrypting signal from a remote controller

1.8.2. Encrypting signal from a remote controller, with the receiver decoder calculating a random number sequence

5 An additional security feature is included in the digital television system by means of the receiver decoder 2020 and the remote controller 2026 operated by the end user. The controller is shown schematically in Figure 3. The controller includes keys 2028. Prior to access of the daughter smartcard 3020 by the receiver decoder 2020, the decoder 2020, under the control of a control
10 means 2030 located in the decoder, transmits an electromagnetic signal to the television screen which in turn displays a four-digit sequence a1a2a3a4, from 0000 to 9999. This may be either a random four digit number, varied at each access of the system by the end user, or a predetermined and constant sequence.

15 Whilst depressing the "MUTE" key 2032, the end user depresses numbered buttons 2034 on the remote controller 2026 corresponding to the sequence a1a2a3a4, and subsequently transmits an electromagnetic signal representing a second four digit sequence c1c2c3c4 corresponding to a personal identification number, or PIN number, of the daughter smartcard 3020. The
20 controller 2026 transmits an electromagnetic signal representing a third four digit sequence, t1t2t3t4, to the receiver decoder 2020. Digit t1 in the sequence t1t2t3t4 is calculated from the digits a1 and c1 by the expression

$$t1 = (a1+c1)\text{mod}10$$

Similar calculations are made in respect of t2, t3 and t4. The digits c1c2c3c4
25 are hence ciphered so as to safeguard against any interception of the signal transmitted by the controller 2026.

In the receiver decoder 2020, the digit c1' is calculated from t1 and compared

to the value of c1 stored therein. Similar calculations are made in respect of c2', c3' and c4'. The as-calculated four digit sequence c1'c2'c3'c4' is compared to the sequence c1c2c3c4 stored in the decoder 2020. If the sequences match, then access to the system is granted; if not, access is
5 denied.

As an alternative, the sequence a1a2a3a4 may be transmitted by the decoder 2020 to the controller 2026, which then transmits t1 to t4, based on the received a1 to a4 and the number c1 to c4 entered by the end user, to the decoder.

10 **2. INTERACTIVE TELEVISION SYSTEM**

The digital television system 1000 may also function in an "interactive" mode, allowing the user to interact with various applications. Figure 5 shows the general architecture of the interactive television system 4000 of the digital television system 1000 of the present invention.

15 **2.1. System Overview**

The interactive system 4000 allows an end user to, for example, buy items from on-screen catalogues, consult local news and weather maps on demand and play games through his television set.

The interactive system 4000 comprises in overview four main elements:

20 an Authoring Tool 4004 at the broadcast centre for enabling a broadcast supplier to create, develop, debug and test applications;

an Application and Data Server 4006, also at the broadcast centre, connected to the Authoring Tool 4004 for enabling a broadcast supplier to prepare, authenticate and format applications and data for delivery to the
25 multiplexer and scrambler 2004 for insertion into the MPEG-2 transport stream

- 14 -

(typically the private section thereof) to be broadcast to the end user;

a Run Time Engine (RTE) 4008, which is an executable code installed in the receiver decoder 2020 owned or rented by the end user for enabling an end user to receive, authenticate, decompress, and load applications into the
5 working memory 2026 of the decoder 2020 for execution. The engine 4008 also runs resident, general-purpose applications. The engine 4008 is independent of the hardware and operating system; and

a modemmed back channel 4002 between the receiver decoder 2020 and the Application and Data Server 4006 to enable signals instructing the
10 Server 4006 to insert data and applications into the MPEG-2 transport stream at the request of the end user.

2.2. Basic Features

The interactive television system operates using "applications" which control the functions of the receiver decoder and various devices contained therein.
15 Applications are represented in the engine 4008 as "resource files". A "module" is a set of resource files and data. A "memory volume" of the receiver decoder is a storage space for modules. An "interface" is used to download modules.

The elements mentioned in the previous paragraph are now described in more
20 detail.

2.3. Applications

An application is defined herein as a piece of computer code controlling high level functions of preferably the receiver decoder 2020. For example, when the end user positions the focus of the remote controller 2026 on a button
25 object seen on the screen of the television set 2022 and presses the validation key, the script associated with the button is run.

An interactive application proposes menus and executes commands at the request of the end user and provides data related to the purpose of the application.

5 Applications may be either resident applications, that is, stored in the ROM of the receiver decoder 2020, or broadcast and downloaded into the RAM of the decoder 2020.

A number of such applications are described hereunder.

2.3.1. Initiating Application

10 The receiver decoder 2020 is equipped with a resident initiating application which is an adaptable collection of modules (this term being defined in more detail hereunder) enabling the decoder 2020 to be immediately operative in the MPEG-2 environment. The application provides core features which can be modified by the broadcast supplier if required.

2.3.2. Startup

15 The startup application allows any application, either downloaded or resident, to run on the receiver decoder 2020. This application acts as a bootstrap executed on arrival of a service in order to start the application. startup is downloaded into RAM and therefore can be updated easily. It can be configured so that the interactive applications available on each channel
20 can be selected and run, either immediately after downloading or after preloading. In the case of preloading, the application is loaded into the memory 2026 and is activated by the startup when required.

2.3.3. Program Guide

25 The Program Guide is an interactive application which gives full information about programming. For example, it may give information about, say, one week's television programmes provided on each channel of a digital television bouquet. By depressing a key 2028 on the remote controller 2026,

the end user accesses an add-on screen, overlaid on the event shown on the screen of the television set 2022. This add-on screen is a browser giving information on the current and next events of each channel of the digital TV bouquet. By depressing another key on the remote controller 2026, the end user accesses an application which displays a list of information on events over one week. The end user can also search and sort events with simple and customised criteria. The end user can also access directly a selected channel.

2.3.4. Pay Per View

The Pay Per View Application is an interactive service available on each PPV channel of the digital TV bouquet in conjunction with the conditional access system 3000. The end user can access the application using a TV guide or channel browser. Additionally, the application starts automatically as soon as a PPV event is detected on the PPV channel. The end user is then able to buy the current event either through his daughter smartcard 3020 or via the communication server 3022 (in the latter case by voice communication). The application may be either resident in the ROM of the decoder 2020 or downloadable into the RAM of the decoder 2020.

2.3.5. PC Download

On request, an end user can download computer software using the PCdownload application. A particular technical problem to be solved is that the computer to which it is ultimately desired to download the software will have a different rate of data input from the rate at which it is broadcast. For example, the difference may be from 9 kbits/second to 1000 kbit/second, with the software being transmitted via the MPEG-2 stream at, say, 500 kbits/second.

In the broadcasting centre, the software is split into N blocks and then inserted into the MPEG private section.

The receiver decoder 2020 includes a bitmap which describes all of the

software blocks. When the downloading is commenced, every bit in the bitmap is set to zero.

The steps in the downloading procedure are:

- read the block number;
- 5 if bit=0 send block to the receiving computer; and
- the receiving computer checks the block and sends an acknowledgement as appropriate.

The receiving computer requires its own software, usually provided on a floppy disk, to join the various blocks of the transmitted software.

10 **2.3.6. XOR table for calculating missing module values**

Problems can arise if a block is lost. A solution to this problem is to use the concept of residency using a XOR function. Additional redundant blocks are added to the data stream from which the values of lost blocks can be derived if necessary.

15 **2.3.7. Auto-interleaving of blocks in successive cycles of a PC download**

Auto-interleaving provides a measure of flow control. Given that the broadcast data rate cannot be altered, the blocks in successive cycles are auto-interleaved. According to the bit rate of the receiving computer, in successive
20 cycles of a carousel every, say, third or fourth block is transmitted to the decoder until all the blocks have been received.

2.3.8. Magbrowser

The magbrowser application comprises a cyclic video broadcast of images with end user navigation via on-screen buttons.

- 18 -

Other possible applications include quiz, teleshopping, telebanking and an internet browser.

2.4. Resource Files

Applications are stored in memory locations in the receiver decoder 2020 and
5 represented as resource files. The resource files comprise panel files, class files, script files and application files.

The panel files describe the screens, the man-machine interface of the application. The class files describe the data structures handled by the application. The script files describe the processing operations of the
10 applications. The application files provide the entry points for the applications.

The applications constituted in this way can use data files, such as icon library files, image files, character font files, colour table files and ASCII text files. An interactive application can also obtain on-line data by effecting inputs and/or outputs.

15 The engine 4008 only loads into its memory those resource files it needs at a given time. These resource files are read from the panel, script and application files; class files are stored in memory following a call to procedure "load_module" and remain locked there until a specific call to the "unload_module" unloading function is made.

2.5. Modules

With reference to Figure 6, a module 4010, such as a tele-shopping module, is a set of resource files and data comprising the following:

- a single application file 4012;
- an undetermined number of panel files 4014;
- 25 an undetermined number of class files 4016;

- 19 -

an undetermined number of script files 4018; and

where appropriate, data files 4020 such as icon library files, image files, character font files, colour table files and ASCII text files.

5 The concept of modules 4010 together with the concept of downloading small pieces of code allows the easy evolution of applications. They can be downloaded into permanent FLASH memory of the decoder 2020 as resident software or broadcast in order to be downloaded into the RAM of the decoder 2020 only when needed by the end user.

10 ***2.5.1. Downloading modules preceded by searching a directory module within a specified local address***

This is a particular feature provided by the present invention.

2.6. Memory Volume

15 A memory volume is a storage space for modules 4010. Such storage spaces are located in the memory 2026 of the receiver decoder 2020. With reference to Figure 7, the decoder 2020 is divided into a RAM volume 4022, FLASH volume 4024, and ROM volume 4026.

20 The RAM volume 4022 in turn is divided into a zone dedicated to firmware, a working space for the engine 4008 and the buffers. The FLASH and other non-volatile memory can be accessed either by an application or the engine itself through a device manager (described hereunder).

Each volume contains a list of modules 4010, each module 4010 containing a list of files 4012, 4014, 4016, 4018, 4020. A module name is unique within the set of three volumes, and a file name is unique within a volume. It is thus possible to have two files bearing the same name, but only when these are
25 located in distinct modules. Except for certain files containing bitmaps, the

contents of all files are compressed in LZW format.

2.6.1. Controlling memory occupation of loading

An application can open any file in any module 4010 in read only mode using procedure "open_df". The read is carried out using procedures "read_df",
5 "getc_df" and "get_df". An application can download an entire module 4010 to the RAM volume 4022 using a procedure "ird_rcv_module". It can then activate this module 4010 using a "load_module procedure". It can also save the module in the FLASH volume 4024 using a "backup_module" procedure.

2.6.2. Dynamic re-allocation of buffer memory in the EEPROM

10 The ROM volume 4026 may comprise EEPROM. There is a bitmap in the EEPROM to manage the saving to the FLASH volume in order to make file management secure. One particular feature is the ability to reallocate buffer memory in the EEPROM by changing the area of the memory reserved for the interactive applications system.

15 2.7. Interfaces

A physical interface of the receiver decoder 2020 is used for downloading modules 4010. With reference to Figure 8, the decoder 2020 contains, for example, six downloading media; MPEG flow tuner 4028, serial interface 4030, parallel interface 4032, modem 4034 and two card readers 4036.

20 To download a module 4010 from a carrier signal, a directory accessible on the carrier signal is first downloaded. This directory simply lists the names of the modules 4010 which can be downloaded from the carrier signal. Once this directory has been downloaded, it is possible for the application to download one or more modules 4010. In the case of MPEG flow, the directory is
25 transported in one single MPEG table. Furthermore, one module 4010 is

- 21 -

transported in one single MPEG table. This is also the case with the five other interfaces; the sections of the directory exchanged on the physical carriers have an 8-byte MPEG-like header.

2.8. Authoring Tool

5 The Authoring Tool 4004 comprises a fully integrated application development package, typically implemented through software, running on a UNIX computer workstation at the broadcast centre. With reference to Figure 9, the Authoring Tool 4004 comprises:

10 a user interface generator 4030, comprising a multi-window graphical tool for the creation and modification of the application, which may comprise panels and assets such as buttons, input boxes and icons;

an icon editor 4032 for creating and modifying icons and storage in libraries;

an image editor 4034 for creating and modifying an image file;

15 a palette editor 4036 for creating and modifying a palette of colours;

a compiler 4038 for writing application scripts in a computer language. The compiler 4038 is used to produce "binary p-code like" code (hereafter referred to as "p-code"), a code interpreted by the decoder Run Time Engine 4008. The code is hardware-independent and full-loading of the code is not
20 required to run the application;

a volume editor 4040 for creating a volume (a downloaded unit) from one or more modules 4010 generated by the compiler 4038;

a decoder debugger 4042 for defining and controlling the execution of scripts; and

25 a documentation tool 4044 for providing easy access to a description of all of the functions which can be used to program scripts for application callback procedures.

Once the application has been designed and developed, it can be fully or partly tested so that any modifications may be checked easily.

- 22 -

2.9. Broadcast Application Server

With reference to Figure 10, a Broadcast Application Server 4006 implements a SADA system. Its main function is to broadcast the interactive application and its data on the MPEG-2 streams.

5 An SA processor 4046 receives applications from the Authoring Tool 4004 and schedules applications and related data according to a play list. The processor 4046 reads and executes an application conductor 4048 from external system 4050. The application conductor 4048 comprises a succession of events with a start date and an end date associated with one or
10 more interactive applications. From the commands read, the SA processor 4046 links together applications or data in a set of MPEG-2 tables, called "sessions", which are sent to the DA processor 4052 with the information regarding when and how to broadcast the session.

The DA processor 4052 manages carousels cycling application programs and
15 data. Its main function is the periodic sending of all of the sections of the session to the multiplexer 2004 so that they can be inserted in MPEG-2 transport streams and broadcast via transponder 2012 to the end user's receiver decoder 2020.

A separate TDP processor is in charge of the creation of the MPEG-2 data for
20 the Electronic Program Guide application, their transmittal to a relevant DA processor and the real-time updating of the old data. The TDP processor may drive several DA processors, one for each broadcast supplier.

In order to authenticate the application, the SA processor 4046 uses an RSA
25 CryptoSafe device using a mother smartcard to hold the private key. To access the device and use the key a password is required. This password is

- 23 -

stored in a ciphered file in the smartcard. If the file is not found, the SADA system will continue to function correctly but only for data.

2.10. Run Time Engine

5 With multiple sources of applications and multiple manufacturing sources of receiver decoder 2020, it is important that one application behaves in the same way on every decoder, and each decoder should execute every application in the same, correct manner. With reference to Figure 11, the present invention provides a run time engine 4008 running under the control of a microprocessor and a common application programming interface 4054. They are installed in
10 every decoder 2020 so that all decoders 2020 are identical from the application point of view.

Figure 11 shows the architecture of the engine 4008 for running applications 4056 on a receiver decoder 2020. The engine 4008, described in more detail hereunder, executes interactive applications 4056 and receives events from
15 outside the decoder 2020, displays graphics and text, calls devices for services and uses functions of a toolbox 4058 connected to the engine 4008 for specific computation.

2.11. Presentation Function

20 A presentation function communicating with the engine 4008 administers the presentation of text and graphics to the end user, and the presentation of end user actions to the engine 4008. The text and graphics are overlaid on the display on the television set 2022, and the user may interact with the application 4056 by means of a keyboard. The term "keyboard" includes the remote controller 2026.

2.12. Event interface

All events, whether input to the presentation function by the keyboard or received through an interface pass through the event interface before being processed by the engine 4008.

5 2.13. Toolbox

The toolbox 4058 contains miscellaneous functions used by the engine 4008. These include data manipulation, such as read or write of one bit in a message, copy of a number of bytes from one data structure to another, read or write of a character string, and compression, expansion or comparison of data structures.

The toolbox 4058 also includes information about firmware 4060 in the receiver decoder 2020, such as hardware and software version numbers and available RAM space, and a function used when downloading a new device 4062.

2.14. Devices

15 With reference to Figure 11, each function of the decoder 2020 is represented as a device 4062. When a new device 4062 is created, it can be installed in existing decoders 2020 by downloading the relevant application 4056 from the broadcast centre.

20 This downloading is performed in the receiver decoder 2020 by an application 4056 which checks the hardware and software versions and, if correct, loads the software module representing the new device 4062 and asks a procedure of the toolbox 4058 to install the new device code within the firmware (in FLASH memory). This can provide a flexible and secure installation of new functions within the decoder 2020 without affecting the rest of the software.

Devices can be either local or remote. Local devices 4064 include smartcards, SCART connector signals, modems, serial and parallel interfaces, a MPEG video and audio player and a MPEG section and table extractor. Remote devices 4066, executed in a remote location, can be any of the local devices, except that a port and protocol must be defined.

2.14.1. MLOAD Device

The MLOAD device allows application script to load an MPEG section, a group of MPEG sections or an MPEG table. This device is particularly important because it deals with the MPEG-2 data stream. It extracts sections using a filter comprising a hardware filter and a software filter.

2.14.2 Hardware pre-filter in the MLOAD device for filtering broadcast data; programmable hardware filter

The hardware filter allows the selection of MPEG sections loaded from the incoming MPEG stream data.

The hardware filter operates by means of a demultiplexer chip, avoiding wasting processor power within the main processor. The filtering conditions can be defined up to 8 bytes. The filter comprises a target, and a mask for enabling or disabling each bit of the target.

Further, by means of the software filter, it is possible to select which sections will be brought to the application. The software filter is always programmed after sections already filtered by the hardware filter. The software filter uses 8 consecutive bytes, the position of the first byte being defined with an offset based on the first byte in the section

The MLOAD device can load single sections, complete tables or groups of sections.

- 26 -

2.14.3. *Preceding/following mode*

Loading of data may be carried out in preceding or following modes.

2.15. Device Manager

Device manager 4068 is a common software interface between the application
5 4056 and the specific functions of the receiver decoder 2020. The device
manager 4068 controls access to devices 4062, declares receipt of an
unexpected event, and manages shared memory.

Before using the services of any device 4062, a program (such as an
application script) has to be declared as a "client", that is, a logical access-way
10 to the device 4066 or the device manager 4068. The manager gives the client
a client number which is referred to in all accesses to a device.

A device 4066 can have several clients, the number of clients for each device
4066 being specified depending on the type of device 4066.

A client is introduced to the device 4066 by a procedure
15 Device_Open_Channel(). This procedure gives the client the client number.
A client can have its name taken out of the device manager 4068 client list
with the procedure Device_Close_Channel().

The access to devices 4062 provided by the device manager 4068 uses either:
synchronous access using procedure "device_call", which is a means
20 of accessing data which is immediately available or a functionality which does
not involve waiting for the desired response;

asynchronous access using a procedure "device_io", which is a means
of accessing data which is not immediately available or a functionality which
involves waiting for a response, for example scanning tuner frequencies to find
25 a multiplex or getting back a table from the MPEG stream. When the

- 27 -

requested result is available an event is put into the queue of the engine to signal its arrival.

A procedure "device_event" is a means of managing unexpected events.

2.16. Architecture of the Run Time Engine

5 2.16.1. *Virtual machine approach in the context of a decoder*

The run time engine 4008 is an executable code installed in each decoder 2020 and includes a virtual machine for interpreting and running applications. The engine 4008 is adaptable to any operating system, including a single task operating system (such as MS-DOS).

- 10 The engine 4008 is based on automaton (which take various events such as a key press, to change various states) and contains its own scheduler to manage event queues from the different hardware interfaces. It also handles the display of graphics and text.

- 15 The engine 4008 comprises a code loader to load and download applications 4056 into the decoder memory 2026. Only the necessary code is loaded into the RAM volume 4024 or FLASH memory volume 4026 in order to ensure optimal use. The downloaded data is verified by an authentication mechanism to prevent any modification of an application 4056 or the execution of any unknown application.

- 20 The engine 4008 further comprises a decompressor. As the application code (p-code like code) is compressed for space saving and fast downloading from the MPEG-2 transport stream or via a built-in decoder mode, the code must be decompressed before loading it into the RAM.

The engine 4008 also comprises an interpreter to interpret the application code

and which uses an automaton to update various variable values and determine status changes, and an error checker.

2.16.2. Automaton

5 The main loop of the engine 4008 lies in an automaton. An automaton comprises a transition table and a status variable chart, called "logical channels".

At every turn of the main loop, a procedure is called up to receive external events (such as pressure on one of the remote control keys, reception of an MPEG-2 packet or a message on a serial port) from the event interface.

10 For each detected event, the procedure comprises a message, called an "event", which is put into one of, say, five queues of the engine 4008. Each of these queues corresponds to a priority level 0 to 4.

15 After the call to the event interface, which fills the queues with events, the engine 4008 searches for the queue having the highest priority containing an event. The event is removed from the queue and used to activate the automaton for which it is intended.

20 A panel automaton manages the man-machine interface. It receives query events from the television screen of the end user, and processes such a query by starting to read the corresponding panel file 4014. It then uses the graphic functions of the interface to trace the panel on the screen of the television set 2022.

The end user can use the four arrow keys of the remote control 2026 to move around the panel. Every time that a key is pressed, an event is processed by the automaton panel. When the user validates a choice using the VALID key
25 on the remote control 2026, the code of the event is processed by the panel

- 29 -

automaton, which generates events requesting scripts to be run and sends them to the script automaton.

5 The script automaton receives script execution requests from the panel automaton. When it receives such a request, the script automaton reads the corresponding script file 4018 and loads it entirely into memory. It then starts running the script and does not go back through the main loop for acquiring events and rescheduling until the script is finished or until it encounters a function called rerouting.

10 There are also several downloading automatons whose function is to process the various protocols linked to the different volumes containing applications 4056.

2.16.3. *Dynamic addition of new routers in the automaton*

15 Particular features of the virtual machine are that it can dynamically add new routers, adding extra logical channels, and that it can add extra automaton lines.

It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

20 Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

The Glossary on the following pages provides definitions of terms used herein. The definitions are not intended to impart any limitation on the scope of the invention.

- 30 -

GLOSSARY**Commercial Offer**

One or more television programmes

ECM (Entitlement Management Message)

- 5 A message sent in relation with one scrambled program. The message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program

EMM (Entitlement Control Message)

- 10 A message, or unique address, dedicated to one end user, or a group of end users, only

SAS (Subscription Authorization System)

The Subscription Authorization System sends subscription rights to the daughter smartcard upon request.

Smartcard

- 15 The Smartcard contains the secrets of one or more commercial operators. A "mother" smartcard ciphers different kinds of messages and the "daughter" smartcards decipher the messages, if they have the rights to do so.

SMS (Subscriber Management System)

- 20 The Subscriber Management System (SMS) manages, amongst others, all of the end user files, commercial offers (such as tariffs and promotions), subscriptions, PPV details, and data regarding end user consumption and authorization

- 31 -

Application

An application controls the functions of the decoder and various devices contained therein

Authoring Tool

- 5 An Authoring Tool enables a broadcast supplier to create, develop, debug and test applications

Broadcast Application Server

An Broadcast Application Server broadcasts an interactive application and its data on the MPEG-2 streams.

10 Device

Each function of the receiver decoder is represented as a device.

Device Manager

The Device manager is a common software interface between an application and the functions of the receiver decoder.

15 Interface

An interface is used to download modules.

Memory volume

A memory volume of the receiver decoder is a storage space for modules.

20 MLOAD

The MLOAD device allows an application script to load a MPEG section, a group of MPEG sections or a MPEG table.

Module

A module is a set of resource files and data.

- 32 -

Presentation Function

A presentation function administers the presentation of text and graphics to the end user, and the presentation of end user actions to the run time engine.

5 Resource file

Applications are represented in the run time engine as resource files.

Run Time Engine

A run time engine is an executable code installed in each receiver decoder and includes a virtual machine for interpreting and running applications.

10

CLAIMS

1. Any or all of the novel and inventive features described herein.

ABSTRACT**BROADCAST AND RECEPTION SYSTEM**

The invention includes a mostly conventional digital television system 2000 to transmit compressed digital signals. A multiplexer 2004 receives a plurality of
5 further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 2008 of the broadcast centre via linkage 2010. The transmitter 2008 transmits electromagnetic signals via uplink 2012 towards a satellite transponder 2014, where they are electronically processed and broadcast via notional downlink 2016 to earth receiver 2018.
10 The signals received by receiver 2018 are transmitted to an integrated receiver decoder 2020 connected to the end user's television set 2022. The receiver decoder 2020 decodes the compressed MPEG-2 signal into a television signal for the television set 2022.

A conditional access system 3000 is connected to the multiplexer 2004 and
15 the receiver decoder 2020, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of deciphering messages relating to one or several television programmes sold by the broadcast supplier can be inserted into the receiver decoder 2020.
20 Using the decoder 2020 and smartcard, the end user may purchase commercial offers in either a subscription mode or a pay-per-view mode.

An interactive system 4000, also connected to the multiplexer 2004 and the receiver decoder 2020 and again located partly in the broadcast centre and partly in the decoder, enables the end user to interact with various applications
25 via a modemmed back channel 4002.

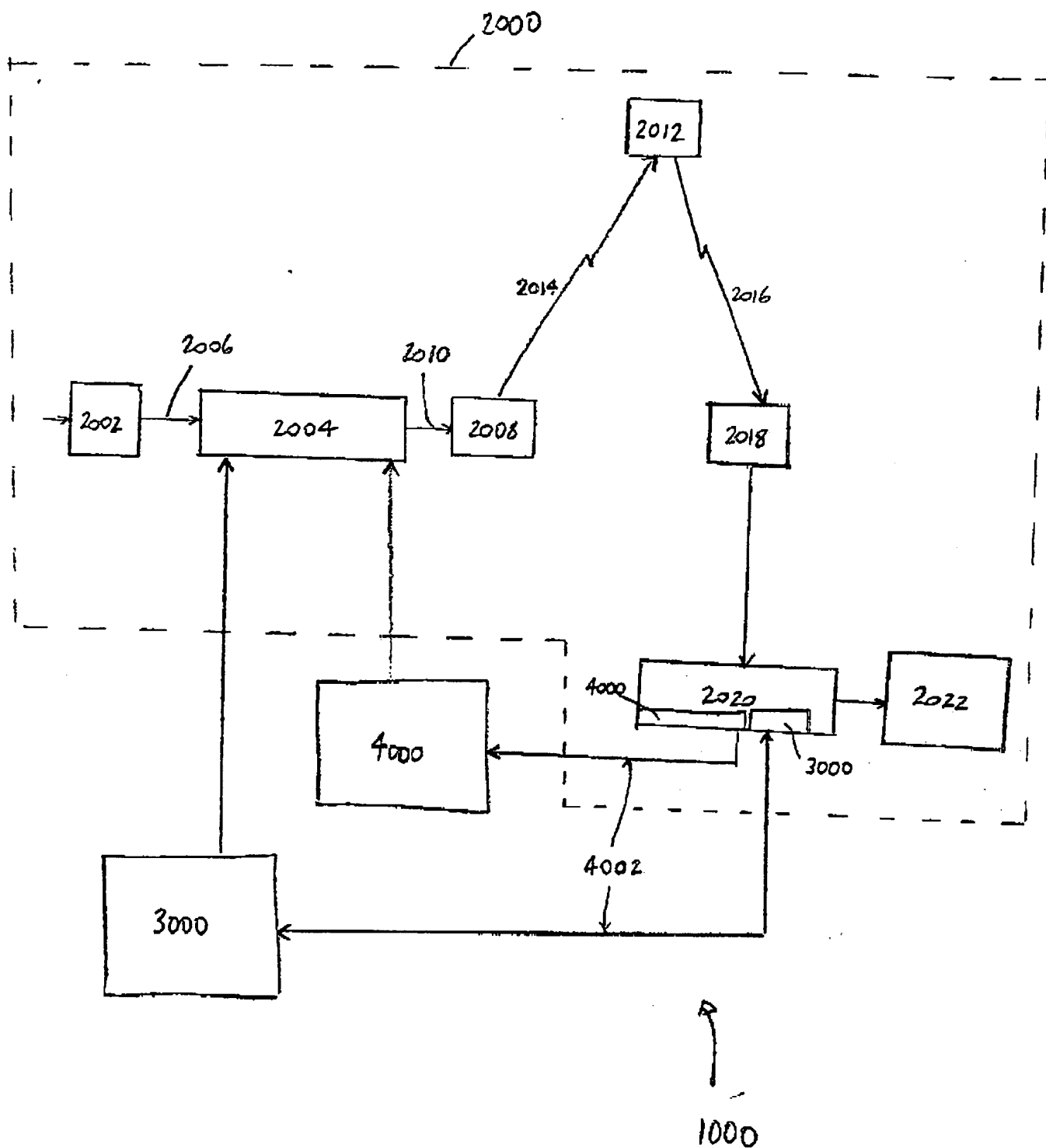


FIGURE 1

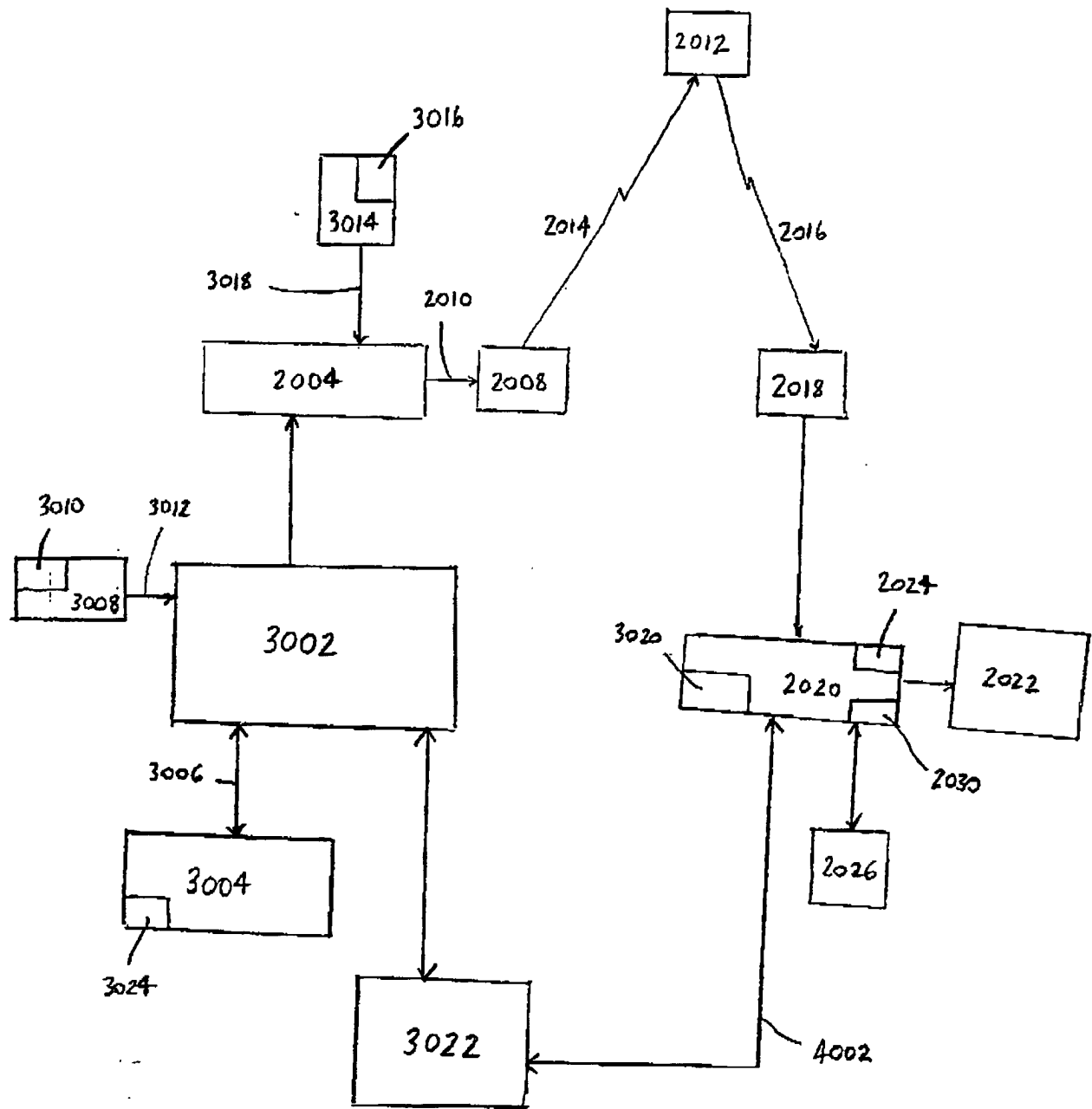


FIGURE 2

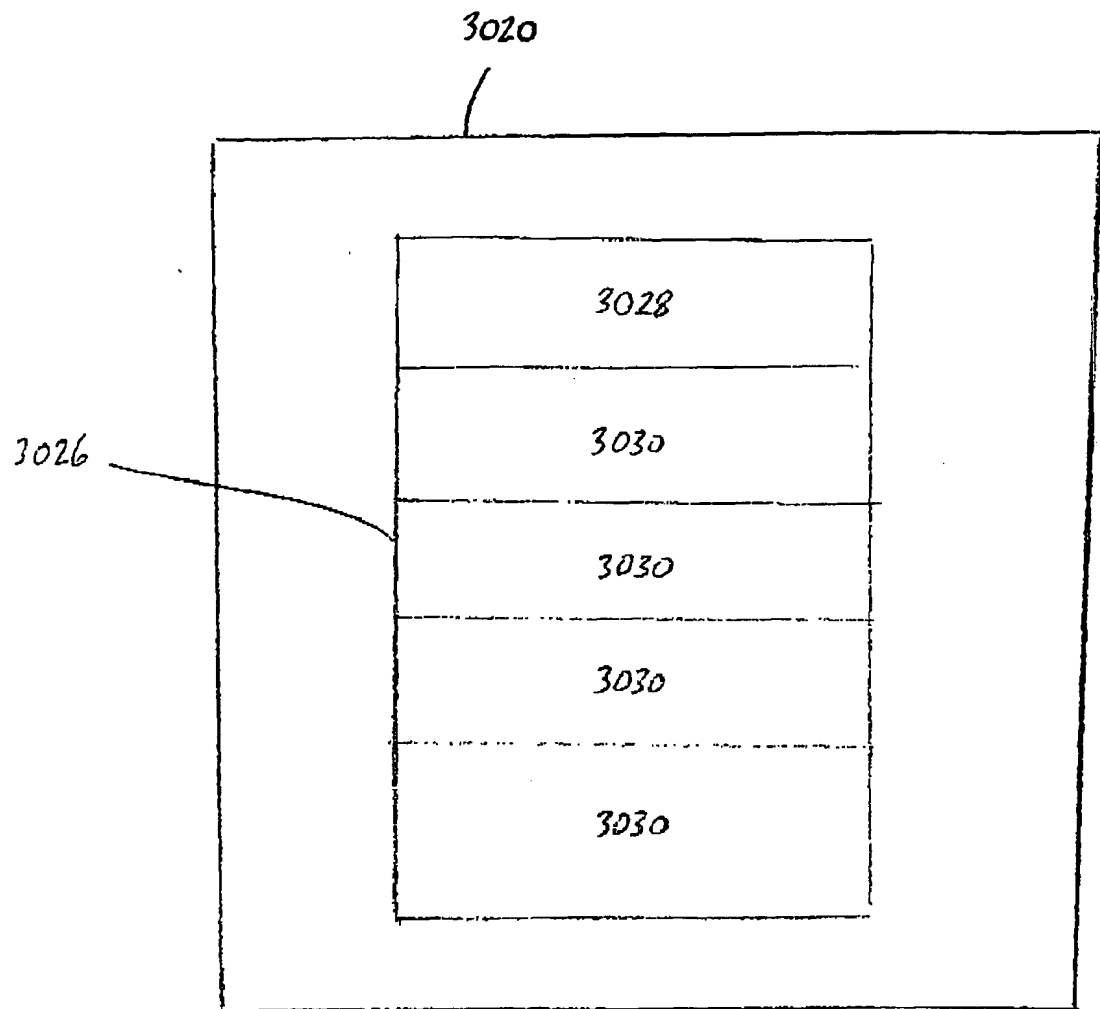


FIGURE 3

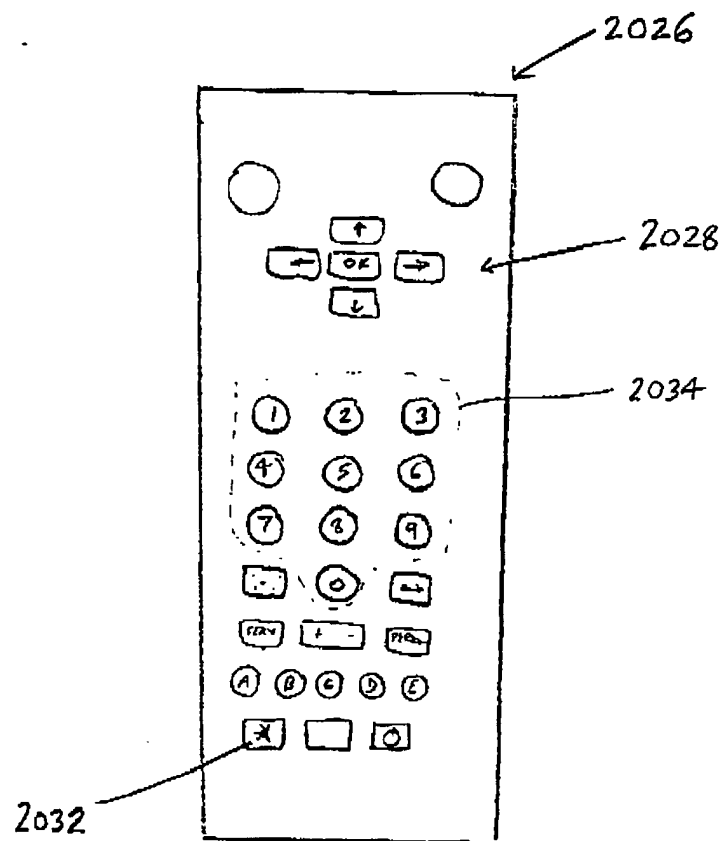


FIGURE 4

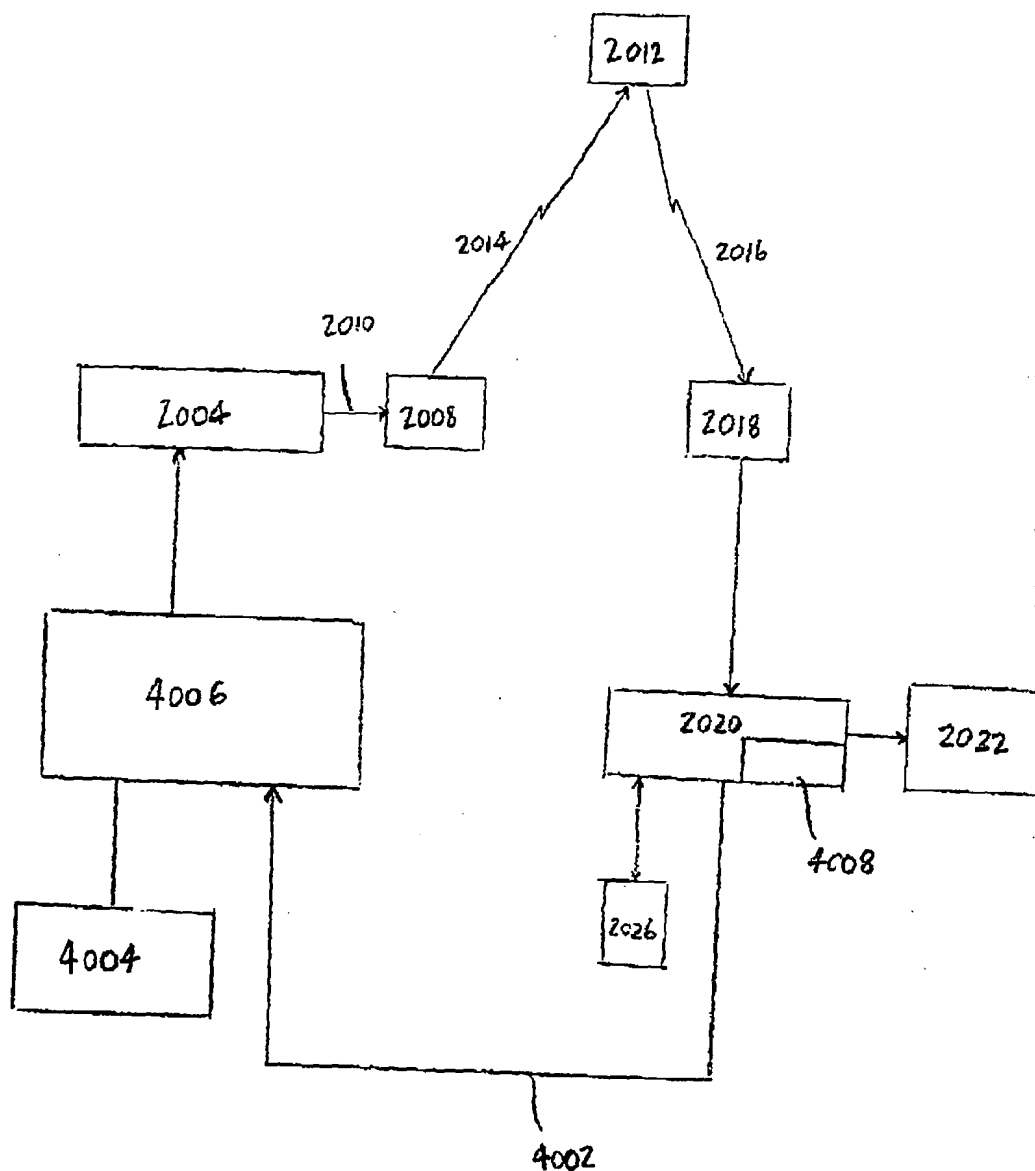


FIGURE 5

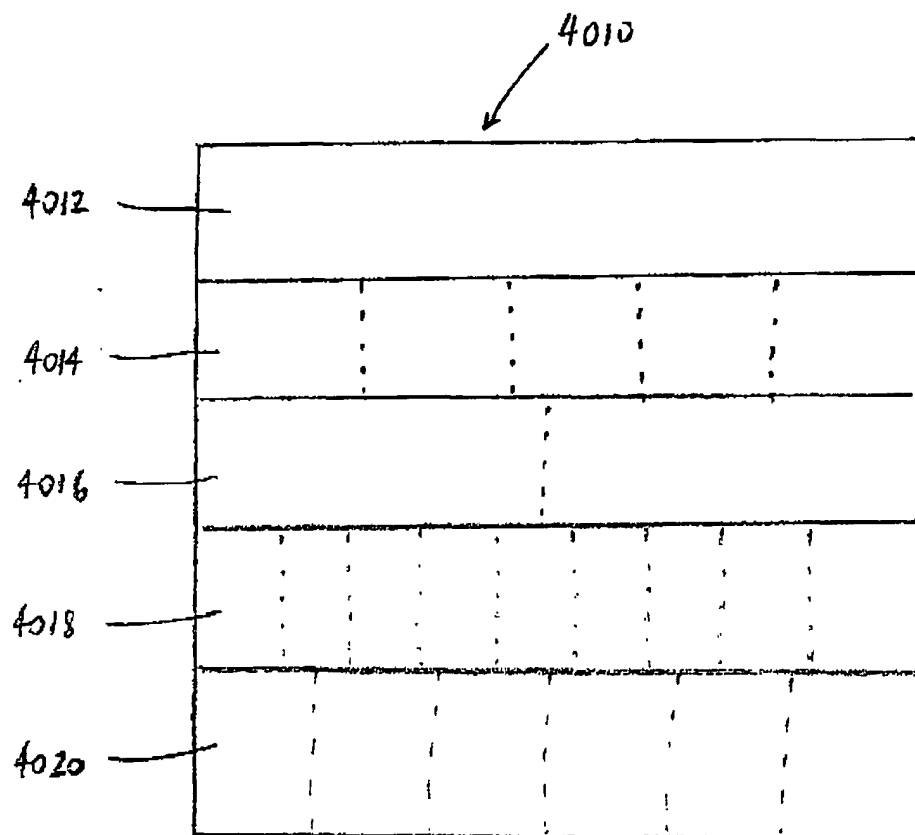
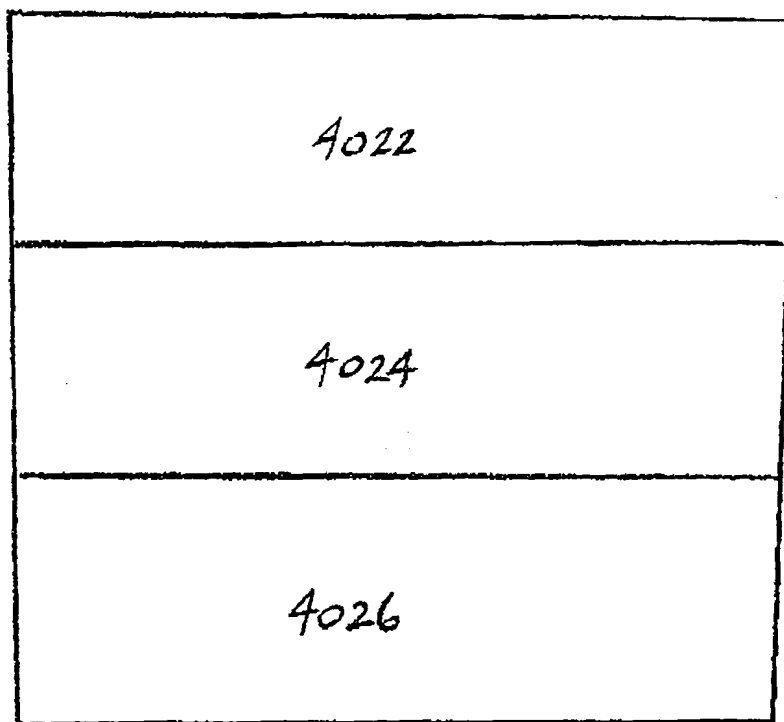


FIGURE 6



2024

An arrow originates from the number '2024' and points upwards towards the bottom box of the stack, which is labeled '4026'.

FIGURE 7

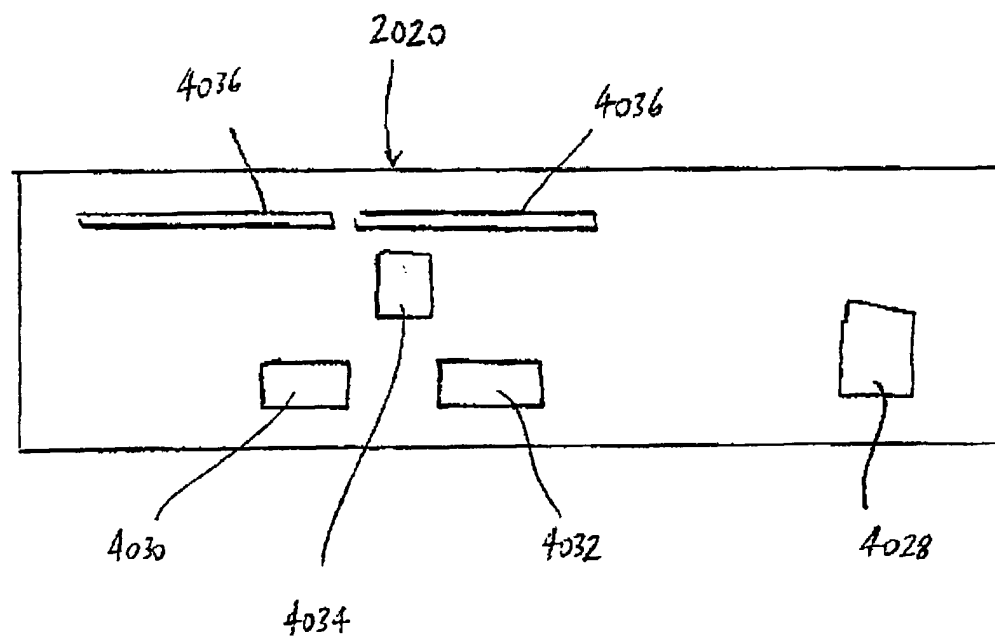


FIGURE 8

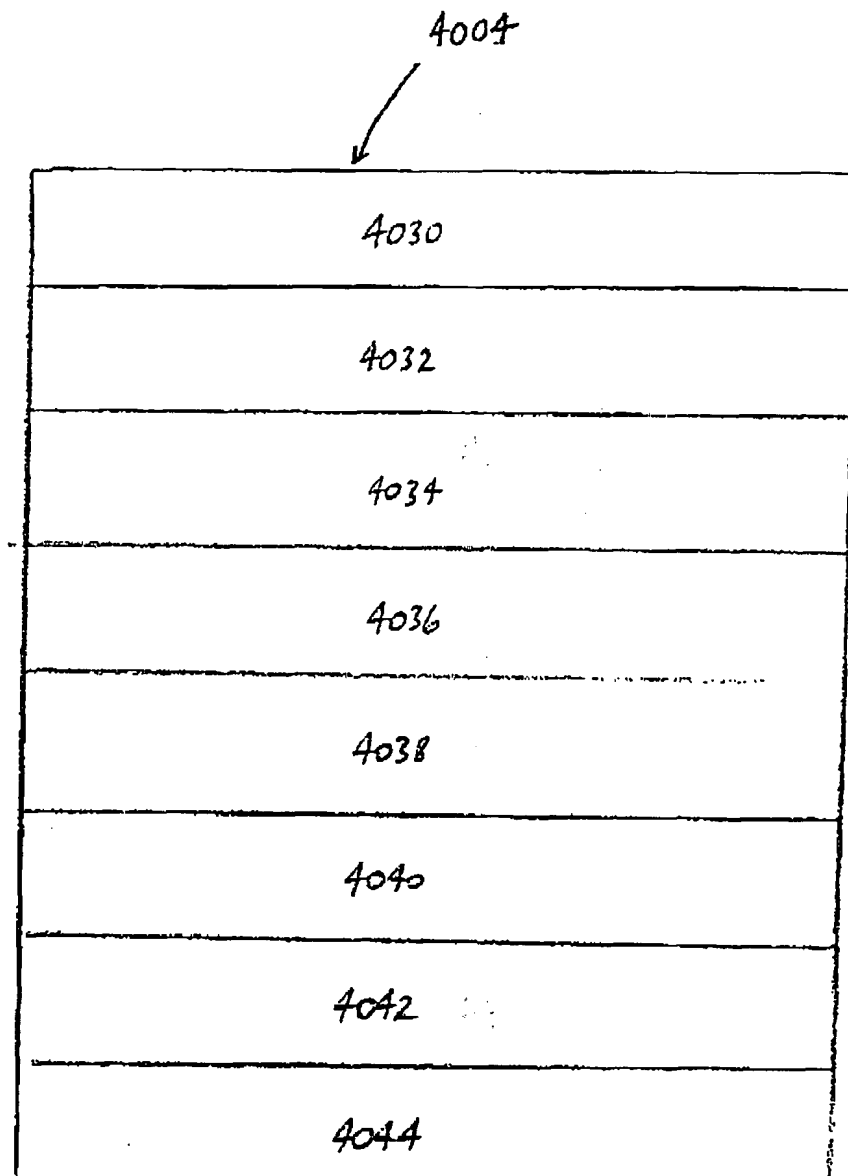


FIGURE 9

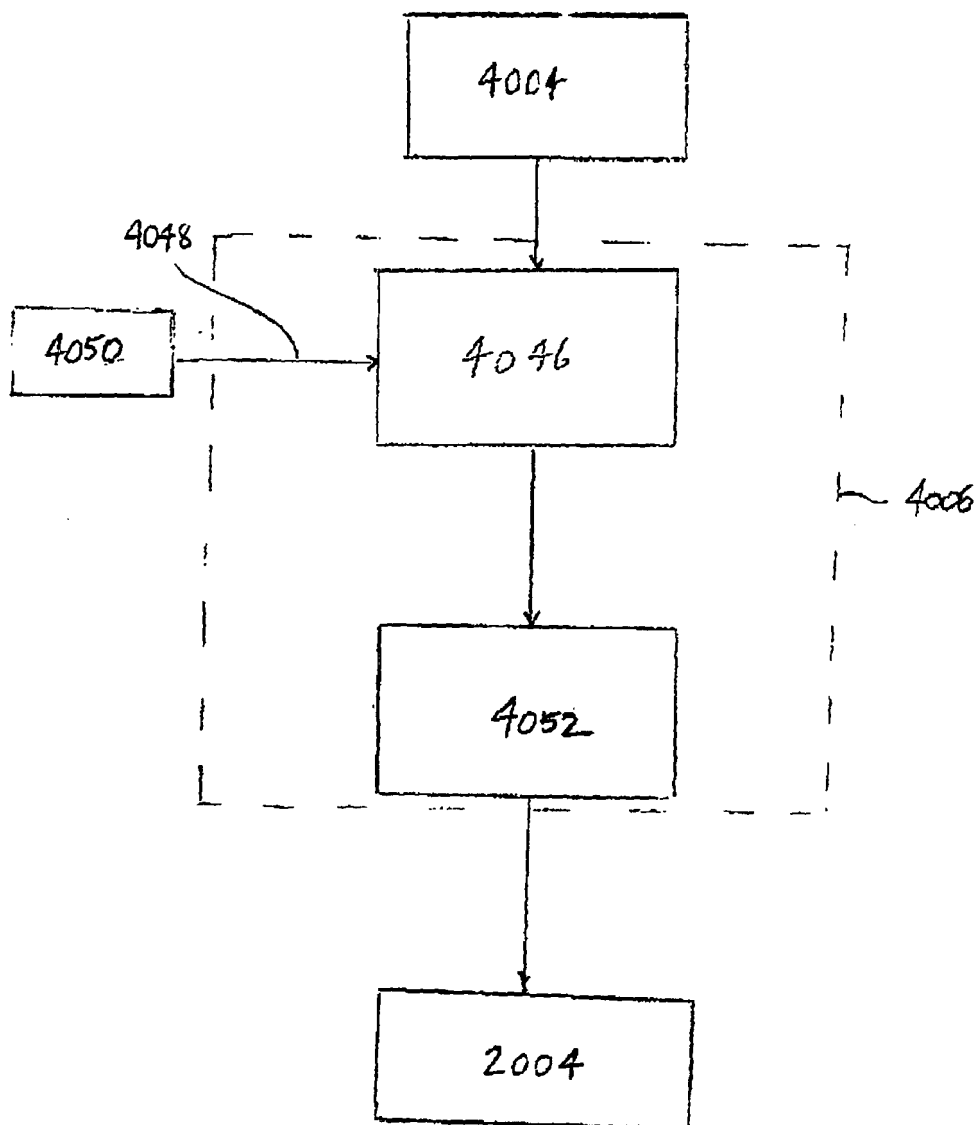


FIGURE 10

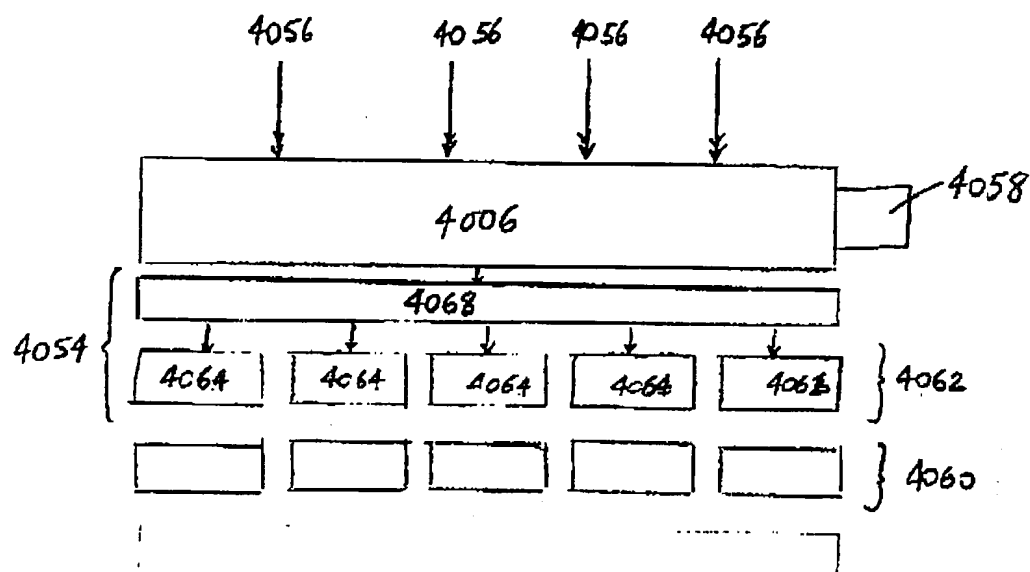


FIGURE 11

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)